小型组织的网络安全

工作人员培养

网络安全工作人员培养的基本方法

- □ **扩大供应渠道。**
  - 贵组织是否与大学和科技学院有关系?
  - 您是否提供网络安全实习或学徒?
- □ **为人才空缺岗位确定并匹配已有供应 。**
  - 您的人力资源部门是否有效地将所需的技能转化为发布的工作描述?
- □ **重新培训现有工作人员，使其成为网络工作人员的一部分。**
  - 贵组织是否正通过将资源转变为网络工作人员利用现有人才?
- □ **通过技术创新降低您的网络工作人员需求。**
  - 您是否与第三方服务提供商签订协议，以形成浪涌能力?
- □ **提高当前工作人员保留能力。**
  - 贵组织是否投资于人才团队成员?
  - 贵组织是否允许有兴趣的个人探究网络安全方面的职业?

确定需求

- □ **明确您的工作量要求。**
  - □ 评估您操作的复杂性以及执行行动需要的速度。
  - □ 考虑浪涌能力需求以及先进技术是否可以有助于减少攻击面。
- □ **明确您的工作人员要求 。**
  - □ 考虑贵公司网络安全工作人员的资格、灵活性和敏捷性。
  - □ 明确理想的汇报结构，并强调哪里更需要多功能人才。
- □ **基于网络安全工作人员支持的业务职能确定他们所需的知识、技能、能力和资格。**
- □ **明确贵组织内现有网络安全工作人员的关键差距。**
  - □ 采用国家网络安全教育计划（NICE）框架等现有工具，指引内部职责和 责任评估。

改善外部招聘

- □ **通过书写清晰且与内部职位相符的职位说明加强职位发布效果。**
  - □ 使用现有工具（例如 NICE 框架）重点强调相关的技能组。
- □ **通过应用程序收集与招聘相关的数据。**
  - □ 系统化整个公司的数据收集和分享，防止形成“孤岛”，并为人才招聘和培养提供支持。
  - □ 定期评估招聘数据，明确人才招揽中存在的缺口。
- □ **依赖多个指标评估候选人的潜能。**
  - □ 考虑实施系统化招聘评估措施。
  - □ 评估相关学位、证书和工作经历。
  - □ 在作出招聘决定时避免依赖一个特定的指标。

促进内部培训和培养

- □ **制定职业生涯发展路线，强调您的网络安全工作人员的晋升轨迹。**
- □ **明确贵组织内对有才能的员工进行再培训和再安排以便担任网络安全职位的路径。**
  - □ 基于兴趣和能力在网络安全中考虑潜在的非传统进入点。
  - □ 扩大技能提升和再培训计划并刺激贵组织内部的转换。
- □ **鼓励内部培训和独立学习。**
  - □ 为继续教育和取得技能证书提供机会。
- □ **追踪工作人员保留数据。**
  - □ 定期评估保留数据，以确认计划是否符合员工需求。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org